AMENDMENTS TO THE SPECIFICATION

Please replace the following paragraphs of the specification. Applicant includes herewith an Attachment for Specification Amendments showing a marked up version of each replacement paragraph.

Please replace the paragraph spanning from page 5, line 12, to page 6, line 2 of the specification as originally filed with the paragraph below:

Accordingly, the hypertext report provides a user interface 128 that may be used by a client when the hypertext document is loaded by a conventional web browser of the type such as Explorer published by Microsoft or Navigator published by Netscape. The user interface 128 when used on a client having a conventional graphical user interface such as Microsoft Windows or Apple Macintosh OS. may appear as a separate window that can be accessed when needed by a user on the client. Using the HTML language it will be appreciated that a number of user interface configurations may be used including, but not limited to, pull-down menus or hypertext listings. Once the document has been sent to the client, no further authentication by the user is required to access the application servers contained in the listing. This user interface provides a great advance over existing, authentication methodologies as the user does not have to provide a separate authentication for each of the application servers. Furthermore, it will be appreciated that the authentication administration can be handled by a single server rather than having separate authentication administration for each of the application servers. The client's communication with the authentication server 111 may include a Secure

Socket Layer (SSL) session link, cookies or other conventional security measures that may be used to verify continued communication from the client to the authentication server.

Please replace the paragraph spanning lines 8-23 of page 7 of the specification as originally filed with the paragraph below:

If the verification is cleared, a Uniform Resource Locator (URL) is generated containing a unique address for the client to access the application and further includes session assignment information that is encrypted by the verification engine prior to transmittal. The special URL is then transmitted to the Authentication Server illustrated by line 140 which in turn forwards the URL directly to the Client illustrated by line 142. Once received by the client, the URL is addressed back to the application server directly from the client along with the encrypted session information initiating the communication link 130. The application server again decrypts the session information and verifies that the URL request was transmitted from the IP address of the client 102 originally transmitted to the application server by the authentication server. The application server also verifies that the session timeout time is still valid. The application server then establishes the trusted communication link 134 directly with the client. The trusted communication link 134 may include security such as an SSL communications link or a cookie containing the relevant session information may be placed on the client's computer. The cookie is used by the application to verify the user and provide other information relevant to the session such as a session time-out information. The URL then redirects the Client to the application page of the web site.